CSP Certification Scheme Summary

Executive Summary

CSP document presents the work performed by the **Cloud Service Provider Certification Working group** (from now on, CSPCERT WG), created on December 2017, from April 2018 to June 2019 in response to the European Cybersecurity Act (EUCA), Title III, which aims to set the grounds to establish an EU-wide framework for cybersecurity certification of ICT services, products and processes, including those services provisioned by Cloud Service Providers (CSP).

The **objective** of the CSPCERT WG is to explore the possibility of developing a European wide **Cloud Certification Scheme** in the context of the **Cybersecurity Act** and to provide the European Commission and ENISA with a set of recommendations that should be taken into consideration when implementing the cloud certification scheme.

The **assurance level** shall be commensurate with the level of the **risk associated** with the intended use of ICT products, ICT service or ICT process, in terms of the probability and impact of an incident.

Scope of the Certification

In order to be certified, the cloud service must meet all the requirements of the certification scheme reference document that are applicable to the service boundary (e.g. SaaS*, PaaS, IaaS, XaaS) and the chosen level of assurance.

***Software as a service** (SaaS) is a model of commercial software exploitation in which these are installed on remote servers rather than on the user's machine.

Assurance levels

A proper risk analysis would define the requirements of a particular level of certification taking into account the benefits versus cost, the risk level and the impact of a cyber incident on the cloud service (**Basic**, **Substantial** and **High**).

Any assurance level assigned to a qualified cloud service through the Cybersecurity Act certification scheme should conduct an **internationally or industry recognized risk analysis**, which should be reviewed as part of the final certification classification.

Even, if it is difficult to foresee all the intended usage of cloud services on a long or even mid-term, it is still possible to consider some tendencies. Thus, it is possible to foresee different levels of

certification required for various kinds of applications, according to the impact of a malicious event that could disrupt it.

Table 1. Example of a selection of a Certification Level of Assurance based on risk scenarios and risk assessment taken by an end-user for a Cloud Service

Area / Risk assessment level priority	Assurance Level of Certification	Example of Data / Services
Personal / low	Basic	Cloud services used to support non-mission-critical or non-safety-critical services, and/or to process, share and store data generated by consumer IoT services and applications, or any other services leveraging open/public/non-sensitive data (e.g. recreational IoT applications - connected lights, games and toys -, home automation without safety impact, video and media streaming, personal web page hosting…)
Personal / moderate and high	Substantial	Cloud services used to support potentially mission-critical or safety-critical services, and/or to process, share and store data generated by consumer IoT services and applications, or any other services leveraging not-public/sensitive data (e.g. IoT applications and home automation with safety issues (heating settings, connected alarms…).
Business / low	Basic	Cloud services used to support business processes which are not substantial or critical for the survival of the enterprise.
Business / moderate	Substantial	Cloud services used to support important processes and/or to process non-mission-critical data. Examples include: ● Telecommunication/telepresence services ● Accounting services ● Payroll services ● Payment services ● Credit card clearing activities ● Security services for Substantial
Business / high	High	Cloud services used to support mission-critical processes and/or to process, share and store sensitive and regulated data. Examples include: ● patents, core systems, ● Intellectual property and data on critical domains that ensure a cutting-edge advantage on the economic scene thus need strong protection against industrial espionage

		• management services on critical infrastructure • Security services for High
Societal/ low and moderate	Substantial	Cloud services used to support business processes/applications and/or to process, share and store data related to sales and e-commerce. General business services to support communication or secure systems.
Societal/ high	High	Cloud services used to support business processes/applications and/or to process, share and store data related to: • Critical Infrastructure (Core financial services being deployed in the CSP) or industrial process and Digital Factory (Industry 4.0, or event 5.0); • Further eIDAS identity services at a High level, that could use cloud computing; • Medical records, which by design needs a high level of security.

Table 2. Cybersecurity act's assurance requirements and their correspondence to the different levels

EUCA Assurance Requirement interpretation	Basic	Substantial	High
Meets the corresponding Security requirements to the assurance level [...]	Yes	Yes	Yes
Designed to mitigate [...]	known basic risks […]	known cyber risks […]	The risk of state-of-the-art cyber attacks
Designed to deter attacker that have [...]	Not applicable	Limited Skills and resources.	Significant skills and resources
Includes technical documentation for review [...]	Yes	Yes (implicit)	Yes (implicit)
Reviews the non-applicability of publicly known vulnerabilities [...]	Not applicable	Yes	Yes
Has implemented the necessary security objectives for the assurance level [...]	Not required	Yes	Yes, at the state-of-the-art
Assessed offer resistance to skilled attackers via penetration testing [...]	Not required	Not required	Yes

Issuance of certificates

An EU-wide cloud service provider security certificate issuer should be using one of the Conformity Assessment Methodologies described in Annex 2.

Typically:

- Certificates issued by a Conformity Assessment Body (CAB), accredited according ISO/IEC 17021 [17], are for an organisation or organisations providing a service, that have chosen to implement a management system for planning, achieving and improving a set of objectives of a particular area of relevance to the organisation (e.g. quality, environment or information security).
- Certificates by a CAB accredited according ISO/IEC 17065 [18] are related to specific products, processes or services, to which the same specified requirements, specific rules and procedures apply. While the provision of a cloud service encompasses more than the manufacture of a simple discrete object, ISO/IEC 17065 [19] equates its applicability of a product to that of a service or process. Related, the General Data Protection Regulation (GDPR) also requires the application of ISO/IEC 17065 for a CAB to perform a conformity assessment.

Maintenance of certificates

The CSP service certification scheme that is being established through the EUCA will become a European Union program that will standardize the way in which cloud computing services are certified within the European Union. The recommended maintenance of those certificates is discussed in this section.

Certifications should be issued by one of the following:

- The National Cybersecurity Certification Authority;
- A delegated authority such as a Certification Body.

Certifications are given to the relevant CSPs in line with the defined Conformity Assessment methodology. Certifications, once issued, should be required to be maintained, at least, in line with such methodology and taking into consideration the aspects listed below:

- CSPs compliance to the certification scheme should be reviewed and/or reassessed in line with the Conformity Assessment methodology.
- The certificates issued should only be applicable to the services agreed by the CSPs and the National Cybersecurity Certification Authority during the conformity assessment process.
- CSPs should be able to update the scope of the certification applicability during the continuous auditing process, i.e. CSPs can add and/or remove services from the scope of the certification assessment.
- CSPs should have the ability to review the assurance levels applicable to them in consultation with the National Cybersecurity Certification Authority. This should be based on changes to products or services offered by the CSPs.
- CSPs should have a right to appeal to the National Cybersecurity Certification Authority, or an authority established by ENISA, for any:
    - Discrepancies generated out of the continuous auditing process;
    - Complaints arising from the outcome of the certification assessment.

- The National Cybersecurity Certification Authority should have a well-defined complaint and enquiry handling mechanism to enable resolutions of concerns and queries from the CSPs.
- Complaints and enquiries should be resolved within a fixed timeframe by the National Cybersecurity Certification Authority, and where required, the National Cybersecurity Certification Authority should engage with the relevant CSP.

Assignment of controls and methodologies for each assurance level

The assignment of controls and methodologies, as noted in Recommendation 26 (namely, the last recommendation in Section 3) should be followed.

This implies that similar security objectives (see Milestone 1 - Annex 1) related to the cloud service certification are shared across assurance levels. Moreover, the **requirements** related to the security objectives described in the Milestone 1 document should be declined in **different** stringency **levels** according to the **assurance levels**. The depth of the evaluation methodologies used and described in the Milestone 2 should also vary according to the assurance level.

The figure below shows how the different controls, corresponding requirements (derived from Milestone 1) and methodologies are declined across certification levels.

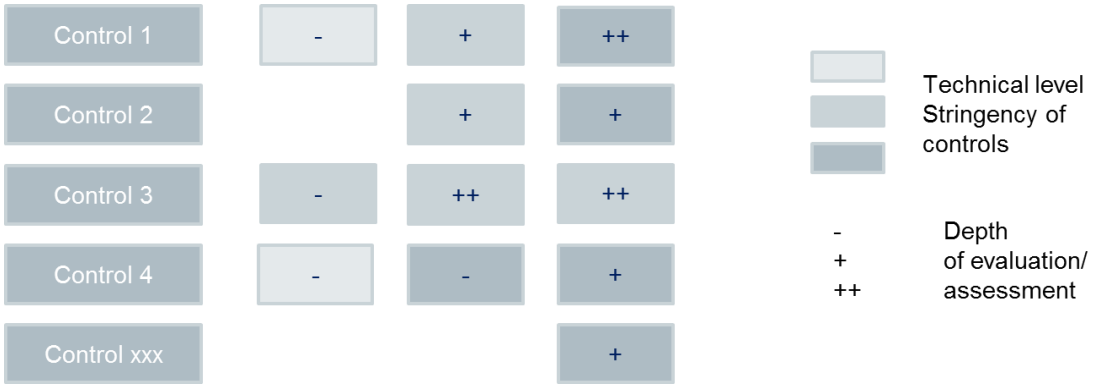

Figure 1. Example of Combination of controls, corresponding Requirements and methodologies.

Further recommendations and explanations regarding the controls and the methodologies are given in Annex 1 and Annex 2 of this document.

Methodology

The methodology followed for the definition of the **security objectives** is detailed below.

The following documents have been used as input sources:

- Study on Certification Schemes for Cloud Computing (SMART 2016 / 0029) [2]
- ISO 27002 [5], 27017 [6], 27018 [7]
- ENISA Cloud Computing Schemes Metaframework (CCSM) [1]
- BSI C5 [4]
- SecNumCloud [3]

During the open consultation, respondents were asked about the adequacy of including further schemes in the analysis such as PCI-DSS [29], Cloud Security Alliance Cloud Control Matrix (CSA CCM) [8], NIST 800 - 53 [11] or any other relevant one that the respondent felt appropriate. While CSA Cloud Control Matrix, SOC2 and PCI-DSS were suggested by many respondents, the following considerations were taken into account:

- Based on the results of previous studies, e.g. [2] on [1] the gaps between the CCM requirements and those included in any of the other control frameworks considered in this analysis (and vice versa) are rather small; for instance the BSI C5 controls are based on the controls of the CSA Cloud Control Matrix in a large proportion; therefore the CCM fully satisfies the security objectives defined in Chapter 3 of this document.
- PCI-DSS [29] is different and could require a further assessment. PCI-DSS has different goals than the other schemes analysed, as it is aimed at a different constituency, so an EU level scheme is not likely to replace it.
- NIST 800 – 53 [11] has a very large number of controls. The mapping analysis available in study on Certification Schemes for Cloud Computing (SMART 2016 / 0029) [11] leads to think that the number of additional security objectives that could be derived is rather small.

The **methodology** to extract the **security objectives** is described next. First of all, the above-mentioned schemes and relevant standards (ISO 27002, ISO 27017, ISO 27018, BSI C5 and SecNum cloud), taking as baseline ENISA CCSM have been **analysed** to seek for commonalities and **families of controls**. In this context, a 'family of controls', namely a domain, is a set of controls focused on a certain aspect, such as network security, operational security, or personnel. For simplification purposes, a family of controls is named as category (labelled as 'EC_Cloudcategory' in the spreadsheet that can be found in Annex 1a).

The **categories of security objectives** are identified are as follows:

1. **Information Security Policies:** ensure the definition of policies related to information security, aligned with the relevant laws, regulations, as well as with the business requirements of the organization. It also includes the definition of the appropriate roles and responsibilities to carry out the implementation of said policies.
2. **Personnel & Training:** Ensure that the employees and contractors are aware and understand their responsibilities towards the information security policies defined and implemented in the organization.

3. **Asset Management:** provide mechanisms for the identification and protection of organizational and information assets, also those coming from customers.
4. **Identity and Access Management:** Put in place the mechanisms to ensure the access to the information, information processing facilities and virtualized environments of only authorized users.
5. **Cryptography and Key management:** Ensure a secure operation of the cloud services with the definition and implementation of the appropriate cryptographic mechanisms.
6. **Physical Infrastructure Security:** Ensure the prevention of unauthorized access to the physical site so as to prevent any damage, loss, failure or theft of any of the business' assets that may hamper the organization's operations.
7. **Operational Security:** Ensure the secure and proper operation of the information security facilities so that the cloud service provider is always operational.
8. **Communications Security:** Ensure the protection of the information in networks, external and internal and in between systems.
9. **Procurement Management:** Define and implement mechanisms to manage the whole supply chain of the cloud service provider and ensure that these procurement activities maintain the appropriate security level.
10. **Incident Management:** Provide the means to manage, react to, and communicate security incidents.
11. **Business Continuity and disaster recovery**: Set out the activities needed to ensure the continuity of the operations of the cloud service recovery, including the disaster recovery ones while ensuring the integrity of the information at all times.
12. **Compliance**: Satisfy the legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.
13. **Security Assessment:** To establish and maintain appropriate procedures for testing key network and information systems underpinning the cloud services and to establish and maintain appropriate procedures to perform security assessments of critical assets.
14. **Interoperability and Portability**: Provide means that allow customers to interface with other cloud services and/or if needed port to other providers offering similar services in a secure way.
15. **System Security and Integrity**: Put in place the appropriate measures to ensure that the system maintains an adequate level of security and integrity in its entire lifecycle, from development to operation, from internal developments to outsourced ones, using both commercial and open source software.
16. **Change and Configuration Management:** Establish and maintain change management procedures for network and information systems.
17. **Risk Management:** Provide the means to ensure an appropriate governance and risk management framework, as well as mechanisms to identify and address risks for the security of the cloud services

CSAR Coverage Cybersecurity Act requirements regarding the CSP certification

	EU Cybersecurity Act – Article 54	Compliance art. 54	Notes
(a)	subject-matter and scope of the certification scheme, including the type or categories of ICT processes, products and services	Yes	The purpose of the scheme is to provide the user of cloud services with a statement about its scope, reliability and security in accordance with regulations. The purpose of a Conformity Assessment Certification is to enhance the credibility (or confidence or trust) towards stakeholders of a statement expressed by a cloud service provider (CSP) that its cloud service (including those from sub-service providers) meets the requirements of a predefined set of control objectives and a related set of measures, equivalent to the requirements proposed in Milestone 1 (Details in Annex 1).
(b)	a clear description of the purpose of the scheme and how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme.	Yes	The purpose of the scheme is to provide the user of cloud services with a statement about its scope, reliability and security in accordance with regulations. The purpose of a Conformity Assessment Certification is to enhance the credibility (or confidence or trust) towards stakeholders of a statement expressed by a cloud service provider (CSP) that its cloud service (including those from sub-service providers) meets the requirements of a predefined set of control objectives and a related set of measures, equivalent to the requirements proposed in Milestone 1 (Details in Annex 1).
(c)	references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II of Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;	Yes	Consider the security categories and additional specifications for high- and low-level security objectives provided in the Milestone 1 document (see Annex 1) based on the analysis of existing standards.
(d)	where applicable, one or more assurance levels;	Yes	For CSPs, three levels of assurance based on the outcome of the risk assessment performed, are permitted. These levels are Basic, Substantial and High.
(e)	an indication of whether conformity self-assessment of conformity is permitted under the scheme;	Yes	Purely self-assessment leading to a Statement of Conformity should not be permitted due to the risks arising from the use of cloud computing services. However, the basic assurance level should be founded on an evidence-based conformity assessment as described in Annex 2.
(f)	where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements;	Yes	Specific requirements for Conformity assessment bodies are covered in section 5 and should be adopted as part of the final certification scheme.
(g)	The specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 51 are achieved;	Yes	Annex 1 presents a set of security objectives that should be taken into consideration by ENISA in the final EU-wide certification scheme.
(h)	where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the conformity assessment bodies by an applicant;	Yes	A template has been provided in the 'Annex 4: Template Report CSP Management Assessment' to support this recommendation.
(i)	where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;	Yes	Upon discussion, the recommendation of the drafting team is that no mark or label is applied in the context of this scheme. The principal reason behind this recommendation is the need for a careful risk assessment to be conducted on a case by case basis to determine the need for a High, Substantial or Basic level of assurance under this scheme. The need for this risk assessment implies that labels or marks are likely to be misunderstood or misinterpreted as providing a guarantee of appropriate assurance.
(j)	rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity	Yes	: CSPCERT WG advises to follow the recommendations regarding the monitoring of compliance with the requirements of the EU certificates and the mechanisms to

	certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;		demonstrate it provided in Sections 5.4.2.1, 5.5.5 and 5.6.4 of this document. Moreover, it is advised that each assurance level foresees the implementation of monitoring mechanisms and processes of the issued certificates.
(k)	where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification;	Yes	Sections 4.2 and 4.3 provide a set of recommendations to grant, maintain, and ensure the continuity and the renewal of any given certificate. The recommendations of those sections should be followed, as ENISA issues the final guidance for the certification scheme.
(l)	rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme;	Yes	As mentioned in Annex 4 of this document, as part of the certification scheme, it should be ensured that CSPs obtaining a certification under the scheme
(m)	rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with;	Yes	Consider including as a set of minimum-Security Objectives as those already defined in Milestone 1 document (e.g. section 3.7 'Operational security'). In addition to what OS.7 says from the section 3.7 Milestone document, a CSP should adhere to a vulnerability disclosure process.
(n)	where applicable, rules concerning the retention of records by conformity assessment bodies;	Yes	That the final certification scheme requires a 7-year period for retention of records.
(o)	the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels;	Yes	It is recommended for ENISA to show how the Security Objectives of the adopted EU-wide cloud certification scheme relate to the other existing schemes, when relevant. ENISA should therefore extend the gap analysis following the methodology described in Annex 1, which has been designed to accommodate further schemes, generic or sectoral.
(p)	the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued;	Yes	For High and Substantial offers, with the unique threat landscape of cloud services, it is recommended that continuous auditing is followed by the CSPs or an annual audit of cloud services is performed at minimal.
(q)	the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services or ICT processes;	Yes	For High and Substantial offers, with the unique threat landscape of cloud services, it is recommended that continuous auditing is followed by the CSPs or an annual audit of cloud services is performed at minimal.
(r)	maximum period of validity of European cybersecurity certificates issued under the scheme;	Yes	For High and Substantial offers, with the unique threat landscape of cloud services, it is recommended that continuous auditing is followed by the CSPs or an annual audit of cloud services is performed at minimal.
(s)	disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme;	Yes	A responsible disclosure policy related to the withdrawal of the certificate should be established for the CSP Certification scheme. The right balance should be ingrained within the final scheme, in order to cope with security, intellectual property and the reputation of the CSP. Information related to non-conformities should be included in any audit report, which is shared only between the auditee and the auditor/certification body. The public and stakeholders (e.g. cloud customer, partners, regulators) should have the right to know when a cloud service is NOT longer certified.
(t)	conditions for the mutual recognition of certification schemes with third countries;	Yes	The topic of mutual acceptance of third-party certification schemes outside the EU is a political issue. ENISA, as part of their final recommendation to the Commission, should recommend a governance model for mutual recognition of non-EU third-country cloud certifications.
(u)	where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing European cybersecurity certificates for assurance level 'high' pursuant to Article 56(6). Such mechanism shall be without prejudice to the peer review provided for in Article 59;	Yes	The mechanisms for peer reviewing for the assurance level high are described in the Section 5.2
(v)	format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and	Yes	The cloud service provider should supply and update the supplementary cybersecurity information that is described in Article 55, for all assurance levels.

	updating the supplementary cybersecurity information in accordance with Article 55.		This information should be made available on the CSP provider's website and found easily by the end user and other relevant stakeholders. It is recommended to define a common format for this information, to have them published and linked aside the certificate in a database maintained by ENISA.


www.eurosmart.com


@Eurosmart_EU


@Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 00 | mail eurosmart@eurosmart.com